Council of Europe Cybercrime Convention

Articles 16 and 17:

Expedited preservation of computer data

Candidate number: 337718

Supervisor: Lee A. Bygrave

Delivered on August 7th, 2003

Number of words: 17.456 (max. 18.000)

1/13/2004

Content

1 Introduction

1.1 Problem for discussion

The emergence of cybercrime poses new challenges for law enforcement authorities. New technology makes it possible to commit crimes from anywhere to anywhere in the world at any time. It enables new types of crime[1] as well as the commission of traditional crimes by means of information technology. The consequences of criminal behavior can be more far-reaching than before because they are not restricted by geographical limitations or national boundaries.[2] Countries worldwide need to reach a consensus as to which computer and technology-related activities should be criminalized, and international cooperation is essential when it comes to combating cybercrime.

The Council of Europe has passed the Cybercrime Convention[3] as a first step to harmonize countries' computer crime laws. It is the first legally binding multilateral instrument drafted specifically to address the problems posed by the spread of criminal activity in computer networks.

---

[1] For example, hacking, virus and denial of service attacks

[2] *Council of Europe - Explanatory Report to the Convention on Cybercrime (ETS No. 185),* hereinafter referred to as the Explanatory Report (para 5)

[3] *Council of Europe Convention on Cybercrime (ETS No. 185),* hereinafter referred to as the Cybercrime Convention

The Convention defines a minimum level of cybercrime offences to be recognized in national laws, and aims to provide the necessary criminal procedural law powers to investigate and prosecute offences committed with the aid of computer technology.

From a law enforcements perspective, traditional methods for investigations will often be insufficient in cyberspace. There are usually no fingerprints, witnesses or physical evidence of the offence. Instead there will be evidence like “electronic trails" leading from the victim back to the perpetrator. Such trails may consist of computer data. Examples are recipients and duration of calls, electronic transactions, web sites visited, storage of illegal content, etc.

To ensure that traditional methods of search and seizure remain effective in a volatile technological environment,[4] the Cybercrime Convention provides for the expedited preservation of computer data.[5] This enables law enforcement authorities[6] to request that computer data are preserved and protected from anything that could alter or destroy the data while an investigation is ongoing. To preserve data means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to deteriorate.[7] This applies in practice only to reasonable small amounts of specified data identified as relevant in a particular case.

---

[4] Explanatory Report para 134

[5] The Cybercrime Convention, Chapter 2 Section 2 Title 2

[6] E.g., the police, internal security agencies, criminal investigation units and others

[7] G8 Government-Private Sector High-Level Meeting On High-Tech Crime, Report for Workshop 1: Data Retention Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, Tokyo, 22-24 May, 2001, hereinafter referred to as the G8 Report, available at www.mofa.go.jp/policy/i_crime/high_tec/conf0105-4.thml (accessed 25 July 2003)

The police are often dependant of information from service providers[8] to follow such electronic trails.[9] However, service providers store data by different means, and for variable periods of time. Some service providers do not log any traffic data at all. Sometimes the crime is not discovered right away; it may take weeks, months or even years, for the victim to realize that he has been the target of a crime.

In the mean time, data protection laws may have affirmatively required the destruction of important data before anyone realized its significance for criminal proceedings.[10]

Law enforcement authorities therefore demand data retention for a certain fixed period of time. "Data retention" would require service providers to collect and keep data as a routine matter, such as traffic data or content data related to future communications. The Cybercrime Convention does not address such requirements, but some countries have already passed national laws with such requirements.[11]

This has caused reactions from data protection authorities[12] and privacy interest groups.[13] They recognize that law enforcement authorities have a legitimate need to investigate crimes, but fear that the extensive collection and use of data will jeopardize the protection of personal data and the right to anonymity.

---

[8] Generic term for companies that provides access to electronic communication, i.e. phone companies, mobile operators and Internet Service Providers

[9] Inger Marie Sunde, "IKT-kriminalitet: Etterforskningsmetoder og personvern", n.d., available at http://www.okokrim.no (accessed 25 July 2003)

[10] Explanatory Report para 150

[11] Examples are Denmark and UK, see further section 7.1 below

[12] E.g., the European Data Protection Commissioners (EDPC)

[13] E.g., Electronic Privacy Information Center (EPIC), see www.epic.org and Global Internet Liberty Campaign, see www.gilc.org for further information (accessed 25 July 2003)

They claim that data retention requirements will deprive citizens of their privacy rights, and warns about the unknown effects and potential misuse of extensive surveillance.[14]

It has been claimed that data retention conflicts with fundamental human rights and freedoms, such as Article 8 of the European Convention of Human Rights. The Article protects every individual against arbitrary interference by public authorities in private or family life, including correspondence. Exemptions may be made for prevention of crime or national security, but any interference or measure must be justifiable and proportionate to the purpose it serves. Any requirement for data retention must therefore fulfill certain conditions, and be worth the privacy costs.

If mandatory data storage requirements are introduced, it will directly affect the service provider industry. For the service providers who are required to store the information, the concerns are primarily those of feasibility, practicability and cost. High costs could harm the development of the information society by affecting end-user prices, and the collection and retention of personal information erodes consumers' confidence in doing business on the Internet due to privacy concerns.[15]

This thesis will analyze the Cybercrime Convention's provisions of data preservation and discuss whether they are appropriate and proportional to the purposes they serve, or if data retention should be mandatory.

---

[14] Statewatch, "Surveillance of Communications: data retention to be 'compulsory' for 12-24 months", No 11, May 2002, available at www.statewatch.org/neww/2002/aug/05datafd1.htm (accessed 25 July 2003)

[15] G8 Report

1.2 Scope of Thesis

The new Cybercrime Convention is used as primary point of reference because it is the first legally binding multilateral instrument in the area of criminal laws. This is an area that traditionally has been outside the scope of EU law, and national legislation contain significant gaps and differences which could act as an barrier to effective police and judicial co-operation in the fight against organized crime and terrorism. There is a lot of interest attached to how and to what extent the Convention will aid the harmonization of criminal laws, as this is vital to identify perpetrators of computer-related offences and bring them to justice. There is some uncertainty connected to what the actual requirements of the Cybercrime Convention are, and how the measures will be implemented in national laws.

The storage of different types of communications data ("traffic data") for business purposes and law enforcement purposes is increasingly regulated in national laws due to data protection- and anti-terrorism laws. However, divergence exists between different countries' laws. This is not the ideal situation for law enforcement, as the police work may be hampered because of variation in collection routines and procedures.

Articles 16 and 17 of the Cybercrime Convention – Expedited preservation of stored computer data – ensures that electronic evidence will be available in a certain period of time while investigation is ongoing. The subject for discussion is whether these provisions are an appropriate measure, or if they should be expanded to include data retention.

The central aim is to cast light on the ongoing debate in Europe, including 1) how suitable the different measures will be for law enforcement purposes, 2) how they affect privacy protection requirements, and 3) what effect they will have on the industry itself, and the development of the information society.

There are a number of important issues that will fall outside the scope of this thesis. Substantive law issues will not be covered. Neither will the real time interception of traffic data or search and seizure is an online environment. Furthermore, international cooperation will only be discussed in relation to the preservation-requirements.

The aim is not to present an extensive overview of all possible legal issues relation to the new requirements of data preservation, but rather highlight some important issues in the ongoing debate in relation to implementing the provisions of the Convention in national laws.

1.3 Source material and Method

The primary source of material is the Cybercrime Convention and its preparatory works. In 1989, the CoE published a study and recommendations addressing the need for new substantive laws criminalizing certain conduct committed through computer networks (Recommendation No. R. (89) 9). This was followed by a second study, published in 1995, which contained principles concerning the adequacy of criminal procedural laws in this area (Recommendation No. R. (95) 13). Building on the principles developed in the 1989 and 1995 reports, in 1997, the CoE established a Committee of Experts on Crime in Cyber-space (PC-CY). The new Committee was given the task of drafting a "binding legal instrument" dealing with cybercrime, with particular emphasis on international issues.[16] The preparation of the Convention was a long process; it took four years and twenty-seven drafts before the final version was submitted.

The area of criminal laws are traditionally not very harmonized, so it is difficult to predict how national variations in legislation will affect the implementation of the Convention.

---

[16] Explanatory Report para 11

It appears to be little literature available on how the different articles are to be understood at the time being. The Explanatory Memorandum to the Convention is used to some degree to interprete the different requirements of Articles 16 and 17.

The two articles are examined to what extent they will be able to fulfill their aim, i.e. whether preservation requirements are sufficient for crime investigation, or if there is need to make data retention mandatory

Data retention requirements raise different concerns regarding privacy, and the retention requirements are analyzed to existing legislation in the privacy field. The analysis is limited to the data protection directives within EU, and Article 8 of the European Convention of Human Rights. Literatures regarding data protection and human rights have been important for the discussion of privacy issues in relation to any data preservation or –retention requirements.

Important sources of material are different articles and reports on the ongoing discussion whether data retention should be mandatory.

To highlight the views of the different interest at stake, common statements from different interest groups are cited. Among these are common statements from European law enforcement authorities and data protection authorities, and also common statements from the industry of service providers.

The data preservation- and retention requirements are briefly discussed in relation to the E-commerce Directive (Directive 2000/31/EC), and what impact such requirements will have on the development of the information society.

1.4 Further presentation

Some background material, such as the use of computer data in criminal investigations, is provided in Chapter 2 below. Chapter 3 gives an outline of the Cybercrime

Convention and a presentation of the requirements of expedited preservation and – disclosure of data. Chapter 4 discusses whether preservation requirements are sufficient for crime investigation, or if there is need to make data retention mandatory. Chapter 5 analyses the different requirements in relation to privacy laws, particular the European Human Rights Convention Article 8 and the European data protection directives. Chapter 6 compares the Cybercrime Convention's preservation requirements to the provisions of Directive 2000/31/EC (e-commerce directive). Chapter 7 gives a short summary over current status in Europe and the United States. Chapter 8 lists some of the most imporant discussion topics yet unanswered, and attempts to suggest some possible solutions. Chapter 9 contains some final remarks and conclusions.

2 Some background material

2.1 Tracing computer crimes[17]

Traces and evidence of criminal behaviour online will usually exist, if the police know where to look. Computer networks and service providers will usually keep track of certain types of information, such as traffic data, authorized and unauthorized access attempts, web sites visited etc. Most important to trace a criminal is probably traffic data, which usually contains an identifier as a telephone number or an IP address (see section 2.3 below).

---

[17] See, e.g. Daniel Morris, "Tracking a Computer Hacker", n.d., available at www.cybercrime.gov (accessed 25 July 2003), Inger Marie Sunde, "IKT-kriminalitet: Etterforskningsmetoder og personvern", and James K. Robinson, "Internet as the Scene of Crime" speech at the International Computer Crime Conference, Oslo, Norway, May 29-31, 2000, available at www.cybercrime.gov (accessed 25 July 2003)

But, several challenges exist that may hinder law enforcement's ability to trace criminals operating online. Criminals may hide or "spoof"[18] their Internet Protocol (IP) addresses, or use offshore systems such as satellite phones and foreign web-based e-mail services. The use of anonymous communication services leaves the police without any traces at all.

Computer criminals are often highly skilled (and in some cases, well funded), and have in-depth knowledge of the latest technology. This means law enforcement need to have equally expertise and resources to keep up with the criminals, and successfully investigate and prosecute cybercrime.

2.2 Computer data

Computer data has been defined and categorized in a number of ways. In this thesis, the term will be used of the logging information held by service providers, such as phone calls, web sites visited, e-mails and location from where a person has called. Computer data will cover (at least) the following three types of data:

Traffic data is any data processed in the course of or for the purpose of the transmission of a communication over an electronic communications network. This can be anything from subscriber information, time and duration of calls, recipient information etc. Sometimes location data (see below) are included in the definition of traffic data, and sometimes subscriber data is defined separately as name and address of the user/ subscriber, or any information available (e.g., birth date).

18 To deceive for the purpose of gaining access to someone else's resources (for example, to fake an Internet address so that one looks like someone else)

Location data is where a person is when calling, i.e. the geographic position of mobile users or terminal equipment.[19] This information is necessary to enable the transmission of communication from and to a user without a fixed location, e.g. cellular or satellite networks. Precise location could be useful for e.g. emergency services to be able to send assistance or rescue teams to the person calling, but in this context location data is used as an illustration of the potential to generate a clear description of geographical movements of the user.

Content data can be defined as the information transmitted, such as a conversation (for phone calls), e-mails, file transfers etc. The content of an e-mail could be compared to a letter: the recipients- and senders address would equal traffic data, and the letter itself would equal the content data.[20]

Giving the fast evolving technology and services, it's impossible to give a complete list and qualification of data. An example of some communications data, given by the G8,[21] is provided in Annex I.

2.3 IP addresses

Another type of computer data is Internet Protocol (IP) addresses.[22] Every computer needs an IP address to communicate across the Internet. Each computer is assigned a

---

[19] IMEI (International Mobile Equipment Identity) codes identifies GSM mobile equipment, SIM cards are identified by IMSI (International Mobile Subscriber Identity) codes

[20] Content data will be discussed further below in section 2.7 and section 8.2.1

[21] G8 is an international cooperation between France, United States, United Kingdom, Russia, Germany, Japan, Italy and Canada

[22] See further Roger Clarke, "A Primer on Internet Technology", Version of 15 February 1998, *Additional material, Masters of Law (Oslo: NRCCL, 2003)*

unique address somewhat similar to a street address or telephone number.[23] Generally, users who have fixed Internet connections (cable modems, private companies etc.) have fixed IP addresses. Dial-up Internet providers usually give addresses dynamically from a pool when a user dials in to connect. By searching IP registration databases it is possible to determine who owns an IP address block. [24] Once the network owner is located, the service provider can be contacted for user- and subscriber list for establishing the identity of the person who used the particular IP address at that particular time.[25]

2.4 The role of Service providers

Service providers act as junctions in Internet communications, and possess a lot of information about users, subscriber information and traffic data. Such information is valuable for the police, and service providers therefore have a vital role in the fight against cybercrime.

The term "service provider" is defined in Article 1c of the Cybercrime Convention as "any public or private entity that provides to users its service the ability to communicate by the means of a computer", and "any other entity that processes or stores computer data on behalf of such communication service or users of such service".

The most common known service providers are the phone companies, mobile operators and Internet service providers. However, a there is a wide range of different providers:

---

[23] Under the current system there are four numbers that range from 0 to 255 (example: 86.214.80.63)

[24] IP addresses are distributed in blocks to network providers or private companies. Once an IP address is captured several methods can be used to trace the user. See example of tools to trace users at http://network-tools.com/ (accessed 25 July 2003)

[25] Sophisticated computer break-ins sometimes include an attempt to erase the IP addresses captured by the log files to prevent this type of lookup

small and larger-scale businesses, national and multinational mobile telephony companies, Internet cafés, broadband connections, universities, airports and hotels, free, anonymous/ pseudonymous services etc. The wording "any public or private entity that provides…ability to communicate..." will subsume all of the above under the definition of a service provider, and data retention requirements would apply to all of them.

2.5 Data storage

The collection, registration and storage of data will vary substantially between the different types of service providers. Some service providers need to know more about their users for billing purposes, such as telephone companies that charge different tariffs for their services (e.g., different tariffs for local- and international calls, or different tariffs depending on what time of day it is). Service providers that are based on dial-up access for their users need to record log in and –out for billing. This is not necessary for service providers that offer a flat rate service.[26]

The volume, technical specifications and costs of storage vary between the different business models. The different service providers use significant different systems for data storage. Unfortunately, it was not possible to present a general overview over technical storage methods, as this would go way beyond the scope of this thesis. Concomitantly, the conclusion is that storage methods vary between different service providers. The costs of retaining certain data items under certain models could be fairly low; the same data under different models quite high.[27]

---

[26] EU Forum on Cybercrime, Discussion Paper for Expert's meeting on Retention of Traffic Data, 6 November 2001 (informal working paper prepared by the Commission services), p. 1, available at http://europa.eu.int/information_society/topic/telecoms/internet/crime/wpap1ov/index_en.htm (accessed 25 July 2003)

[27] See further section 8.3.1 below

2.6 Access to stored data

Law enforcement authorities generally have sufficient powers to search and seize relevant materials, subject to restrictions on obtaining certain types of data.[28] To my knowledge, no reports exist of how many computer-related crimes that are solved directly from access to traffic data – or on the other hand, how many cases that remains unsolved because there are no traffic data available.

However, there are a few reports of requests from law enforcement authorities to service providers regarding access to traffic data. In UK, it is estimated that 1 million requests are being made to telephone companies for information. Law enforcement authorities are also requesting information from Internet service providers, but not in such large quantities.[29] In Norway, no reliable statistics are available but law enforcement authorities estimate "a few hundred" each year.[30]

The data most often requested by law enforcement authorities are the name and address associated with a screen name and to a lesser extent the identification of a subscriber by an IP address.[31]

2.7 Is there a difference between traffic and content data?

Some will claim that there is an artificial distinction between traffic and content data. It has been stated that this is an "old-fashioned" distinction, based on old technology

---

[28] For access to communication data in Norway, see Fuhr, Ringdal & Mørkved: "Etterforskning av telekommunikasjon: Loven krever fritak fra taushetsplikten", published in *Juristkontakt* 2/2003

[29] All Party Internet Group (AGIP), "Communication Data: Report of an Inquiry by the All Party Group", January 2003, available at http://www.apig.org.uk/AGIPreport.pdf (accessed 25 July 2003)

[30] Økokrim, July 2003

[31] Rainer Allitsch, "Data Retention on the Internet – A measure with one foot offside?" CRI 6/2002, p. 162

where the only means of telecommunication was the telephone.[32] Today's communication technologies[33] carry voice, sound, video and huge volumes of information data. A person can do several things simultaneously: browse several web sites, send mails, download music etc. The information revealed from this type of communication is likely to be more revealing and sensitive than a phone number called, for example a header containing the URL of website(s) visited or the subject line of an e-mail. Because such "navigation data" show which pages on a website have been visited, they could reveal the actual content of an individual's communication and thereby his or hers' personal interests (e.g. political opinions, religious beliefs, health or sex life).

3 CoE Cybercrime Convention

3.1 Introduction

The Council of Europe Convention on Cyber Crime (ETS No. 185) is, as mentioned above, the first legally binding multilateral instrument drafted specifically to address the problems posed by the spread of criminal activity in computer networks. The Convention aims to reach a minimum level of substantive and procedural provisions in the field of criminal law, and to supplement already existing multilateral and bilateral

[32] Allitsch, p. 164

[33] Communications is accomplished by sending pieces of information called "packets" that include the IP address of the destination computer, the URL of a website or the heading of an e-mail, etc. (packet-switched technology)

agreements between signatory Member States.[34] It is not only an agreement between European states; the intention is to enable the largest possible number of States to become Parties.[35]

Cybercrime can be distinguished in two categories; traditional crimes committed with the aid of computer technology, and new computer specific crimes (i.e. illegal access to computer networks, virus attacks etc). As for the latter, the Convention defines a set of substantive laws that are to be recognized in national laws. The procedural provisions will apply to any offence committed by means of a computer system,[36] irrespective of the nature of the criminal offence.

The Convention is not self-executing, but obliges Contracting Parties to incorporate the Convention's principles into domestic legislation. The Convention is thus typical of the way multilateral law enforcement conventions are drafted. Most substantive and procedural provisions start with "Each Party shall adopt such legislative and other measures as may be necessary…" It is anticipated that parties will fulfill their international obligations consistent with their particular domestic legal systems.

The Convention sets out for minimum standards, and thereby creates a significant leeway for the Member States when incorporating the Convention in national laws. Moreover, Parties are allowed to make significant derogations[37] and reservations.[38] Important issues are left to definition in national law, such as how to obtain expedited

---

[34] See, for example, *the European Convention on Mutual Assistance in Criminal Matters (ETS No 30)* and the *European Convention on Extradition (ETS No 24)*, cf. CoE Cybercrime Convention Art 39

[35] Explanatory Report para 304, 316

[36] Explanatory Report para 19

[37] See, for example, Articles 21(2) and 29(4)

[38] Article 42

preservation and partial disclosure of traffic data when more than one service provider is involved in the communication.

Many of the provisions are diffuse with little authoritative guidance on how they are to be interpreted. The Convention has been issued with an Explanatory Report prefaced with a disclaimer stating, "The text of this Explanatory Report does not constitute an instrument providing an authoritative interpretation of the Convention, although it might be of such a nature as to facilitate the application of the provisions contained therein". Caution therefore needs to be exercised when using the Explanatory Report to interpret the provisions of the Convention.

The Convention does not mandate any particular body to ensure its implementation in national laws. This raises the question what happens if a contracting Party does not implement the necessary measures, or within a given time period. Can a citizen in a contracting Party call upon the Articles in the Convention when the time limit for implementation is due? If the answer is yes, the Convention will have a direct binding effect on the contracting Parties. This is probably not the intention, though, since the Convention allows a number of reservations and derogations, which is explained by "the fact that the Convention covers area of criminal law and criminal procedural law which is relatively new to many States", Explanatory Report para 320. Thus, the main sanction for not conforming to the requirements would probably be the political pressure from other Parties to implement the principles of the Convention in national law.

Article 43 authorizes the Secretary General of the Council of Europe to periodically enquire about the prospect for withdrawal, in order to maintain some pressure on the Parties and to make them at least consider withdrawing their reservations.[39]

---

[39] Explanatory Report para 322

Article 46 provides for the consultations of the Parties for the purpose of facilitating the effective use and implementation of the Convention by the Parties.

3.2 Signatory and Ratification

As of 25 July 2003, the Convention has not entered into force. It has currently been signed by 30 of 44 member states of the Council of Europe, and by 4 non-CoE member states - United States, Canada, Japan and South Africa.[40] The Convention will enter into force when 5 ratifications, acceptances or approvals are received. This figure is higher than the usual threshold (3) in Council of Europe treaties and reflects the belief that a slightly larger group is needed to successfully begin addressing the challenge of international computer- or computer-related crime.[41] So far, 3 CoE States have ratified the Convention.[42] [43]

The Convention is open for ratification by States that are not members of the CoE (Article 36). Once the Convention enters into force, other non-member States may be invited to accede to the Convention in conformity with Article 37, paragraph 1.[44] Invitation of others requires the unanimous consent of the contracting Parties.

---

[40] Status by 25 July 2003

[41] Explanatory Report para 305

[42] Albania, Croatia and Estonia (status by 25 July 2003)

[43] In Norway, the government has appointed a working party to evaluate necessary changes in existing legislation prior to the implementation of the Cybercrime Convention. The working party has submitted its first report in June 2003, and the second report is expected autumn 2003. The first report is not public yet (as of June 2003), but it is expected that Norway will have to pass some new legislation to conform with the requirements of the Convention (Økokrim, June 2003).

[44] Explanatory Report para 304

3.3 Main lines of the Convention

The Convention aims principally at (1) harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international cooperation.[45] The Preamble of the Convention explains the purposes for drafting the Convention and the goals it intends to achieve; Chapter I determines the terms used; Chapter II specifies the measures to be taken at the national level; Chapter III addresses international co-operation and Chapter IV deals with administrative matters.

3.3.1 Offences listed

Section 1 of Chapter II (substantive law issues) covers both criminalization provisions and other connected provisions in the area of computer- or computer-related crime. Dual criminality is often requested in mutual assistance matters, i.e. that the conduct under investigation is a crime in both the requesting and requested countries and is punishable. It is therefore necessary to ensure a minimum of substantial provisions to be recognized in national laws. When one country's law criminalizes computer-related crime and another country's laws do not, cooperation to solve a crime may not be possible.

The Convention first defines 9 offences grouped in 4 different categories, and then deals with ancillary liability and sanctions. The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference,

[45] Explanatory Report para 16

misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighboring rights.[46] An Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist or xenophobic nature committed through computer systems (ETS 189) has been drawn up, because it was not possible to reach consensus on the criminalization of such conduct within the Convention itself.[47]

3.3.2 Procedural law

In addition to substantial law statutes, appropriate procedural law provisions are necessary to investigate computer-related crime, both at the national level and internationally. Section 2 of Chapter II (procedural law issues) determines first the common conditions and safeguards, applicable to all procedural powers in this Chapter. The safeguards ensure the compliance with the principle of proportionality and with adequate protection of human rights and liberties (see further below, section 3.4.2), then sets out the following procedural powers: expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data and interception of content data. Data preservation is a new legal power for most countries, [48] and will be dealt with in further detail below.

3.3.3 International co-operation

Since computer-related crimes may be committed from anywhere, or criminals may use service providers in different countries to hide their tracks, international police and

---

[46] Explanatory Report para 18

[47] See Explanatory Report to Additional Protocol (ETS 189) para 4

[48] Explanatory Report para 155

judicial co-operation is often required. In addition to the traditional forms of international cooperation, covered by such texts as the European conventions on extradition and on mutual assistance in criminal matters,[49] the Cybercrime Convention will enable law enforcement authorities in one country to collect computer-based evidence for police in another. However, law enforcement authorities may not conduct transborder investigations or searches. The Convention aims for international co-operation to "the widest extent possible".[50] One of the most important new measures is the establishment of a 24/7 contact network, operating round the clock and seven days a week, to provide immediate assistance with current investigations.[51]

3.3.4 Jurisdiction

The transnational nature of many communications network raises complex issues relating to the exercise of law enforcement powers across multiple sovereign jurisdictions. While cybercrime may be global in nature, national boundaries exist for law enforcement. In the case of crimes committed by use of computer systems, there will be occasions in which more than one country has jurisdiction over some or all of the participants in the crime.[52] Concepts like "place of origin", "where the harm occurred" and "closest connection" may be difficult to determine. The participating countries must establish jurisdiction for any computer-related crime committed on their territory, or by their nationals. The aim is to avoid cybercrime havens. Article 22 explicit lists that contracting Parties need to establish jurisdiction on board of ships or

---

[49] *The European Convention on Extradition*, opened for signature in Paris, on 13 December 1957 (ETS No. 24) and *the European Convention on Mutual Assistance in Criminal Matters*, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30)

[50] Article 23

[51] See Article 35 of the Convention, and further the Explanatory Report para 298-302

[52] Explanatory Report para 239

aircraft under their laws. The reason is probably to avoid "virtual countries" that are created on ships or on aircrafts constantly moving through networks and outside any country's jurisdiction.

3.3.5 Participating countries

The CoE's member states drafted the text together with Canada, USA, Japan and South Africa. Because the provisions in the Convention at the drafting stage generally were adopted by consensus rather than by member state vote, the non-CoE member states had a real voice in the drafting process. By virtue of their having participated in the Convention's elaboration, the countries mentioned also automatically had the right to become parties to the Convention.

3.4 Procedural powers

3.4.1 General

Chapter 2 Title 2 of the Convention provides for the expedited preservation of stored computer data and partial disclosure of traffic data. Expedited preservation of data ensures that traditional measures for collection of evidence, such as search and seizure, remain effective in a constantly changing technological environment.[53] With a few keystrokes, or by operation of automatic programs, evidence may be deleted, altered or moved, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt.[54] The Convention requires signatory countries to enable law enforcement authorities to request preservation of already identified data, on a case-by case basis.

---

[53] Explanatory report para 134

[54] Explanatory Report para 282

Preservation of data is not a new idea; it has been in the law of for example the United States for several years. 18. U.S.C. 2703 (f)[55] requires an electronic service provider to "take all necessary steps to preserve records and other evidence in its possession pending an issuance of a court order or other process" upon "the request of a governmental entity." This applies in practice only to reasonable small amounts of specified data identified as relevant to a particular case where the service provider already has control over that data.

There are no requirements in the Convention for service providers to collect data that has not yet come into existence; neither does the Convention require any particular architecture or capability to be in place. In other words, the Convention does not expect a service provider to be able to obtain evidence that it is not technically capable of collecting.

The drafters of the Cybercrime Convention discussed whether the Convention should impose an obligation for service providers to routinely collect and retain data for a certain fixed period of time, but did not include any such obligation due to lack of consensus.[56]

However, while there are no mandatory technical retention requirements placed upon service providers, contracting Parties may impose such obligations under their legal system. As will be shown in Chapter 7, several EU member states have passed legislation that makes data retention mandatory.

---

[55] Full text available on http://www.usdoj.gov/criminal/cybercrime/usc2703.htm, (accessed 25 July 2003)

[56] Explanatory Report para 135

3.4.2 Conditions and safeguards

Articles 14 and 15 contain important instructions on the scope of procedural provisions and what conditions and safeguards must be in place. Legislative and other measures as may be necessary to establish in national laws are subject to, and shall be in accordance with the principle of proportionality (Article 14), and shall provide adequate protection of human rights and liberties (Article 15). The principle of proportionality is central in EU law.[57] Any interference of rights, responsibilities and interests of individuals or third parties, must be justifiable and proportionate to the purposes served. Applied to crime investigation, it means that any interference of such rights must be proportional to the nature and circumstances of the offence, with consideration of public safety on the one hand and the protection of the individual on the other.

3.4.3 Definition of terms

Article 1 provides the definition of a few of the terms used in the Convention. Important to note, the definitions are very broad. E.g., "computer data" is defined in Article 1(c) of the Convention as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function".[58] This definition would cover all types of data as described in section 2.2 above.

"Traffic data" may be subsumed under the definition of computer data, but has a separate definition as "any computer data relating to a communication by means of a computer system that formed a part in the chain of communication, indicating the

---

[57] See further Takis Trimidas, *The General Principles of EC Law,* (New York: Oxford University Press, 1999)

[58] The Explanatory Report para 25 adds that the definition of computer data builds upon the ISO-definition of data. This definition contains the term, "suitable for processing".

communication's origin, destination, route, time, date, size, duration or type of underlying service".

The definition of "Service provider" is already discussed in section 2.4 above.

3.5 Article 16 - Expedited preservation of stored computer data

The scope of Article 16 is to ensure that national competent authorities are able to order or similarly obtain stored computer data, before they are destroyed, in connection with a specific criminal investigation or proceeding.[59] The Article applies at national level; see section 3.8 below for measures at the international level.

Article 16 reads:

> *1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.*
>
> *2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.*
>
> *3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.*
>
> *4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.*

[59] Explanatory Report para 158

According to Article 14, all the powers and procedures required to be established in Section 2 of the Convention are "for the purpose of specific criminal investigations or proceedings", which limits the application of the measures to an investigation in a particular case. The preservation requirement applies in practice only to reasonable small amounts of specified data identified as relevant in a particular case.

3.5.1 "Preservation"

The term "preservation" is not defined in the Convention.[60] Neither does the Convention give any guidance on how the preservation is supposed to be carried out, and leaves it for national legislation to specify technical means. Article 16(2) provide for measures to "maintain the integrity". This would probably keep it safe from any risk of destruction of the data. Preservation would further imply measures to ensure the confidentiality (se further section 3.5.5 below) and integrity of the data.

3.5.2 "Expedited"

The Convention provides for "expedited" preservation (Article 16) and disclosure (Article 17). The term is not defined, but could in my opinion be understood as "without undue delay".[61] This interpretation is supported by the reference to "in particular where there are grounds to believe that the computer data is particular vulnerable to loss or modification", Article 16(1), i.e. when there is a need for a quick response.

---

[60] See Section 1.1 for the definition of "preservation" posed by the G8 Report

[61] Foundation for Information Policy Research (FIPR) comments in that this could mean that data was shipped abroad only few minutes after it was collected, "Communication Data: Report of an Inquiry by the All Party Group (AGIP)", January 2003 (para 194). See www.fipr.org and http://www.apig.org.uk/ for further details (accessed 25 July 2003)

3.5.3 "In… possession or control"

The term "in the person's possession or control" in Article 16(2) refers to information that already exists, and that the person in question has access to it or owns the information. It may be data stored at the person's computer, or at another location (at work) but where the person in speak controls access to it. A question is *when* traffic data exist in a country, or a person has access to it. Multi-national service providers may have established centralized systems abroad, and the communication data could be transferred hereto.[62] The question will not be elaborated further here. The Explanatory Report suggests in para 173 that the term "possession or control" refers to physical possession of the data concerned, and situations in which the data to be produced is outside the person's physical possession but the person can nonetheless freely control production of the data (for example at a remote storage facility provided by another company.

3.5.4 Preservation period

The preserved data may be stored for a period of time as long as necessary, up to a maximum of 90 days (Article 16(2)). Within this period the police must have achieved the necessary authorizations to access the information. A Party may provide for the period to be renewed, if necessary. The Convention does not give any guidance on how many periods the renewal may be granted, and leaves it for national legislation to decide. Important to note, the Convention gives no guidance as to what happens with the preserved data after the storage period, if no authorization to access the data has

---

[62] Privacy laws may impact the transborder transfer of personal data. See, for example Directive 95/46/EC Article 25; note the exemption in Article 26(1)(d). For further details, see Lee A. Bygrave, *Data Protection – Approaching Its Rationale, Logic and Limits* (The Hague/Boston/London: Kluwer Law International, 2002), pp. 79-84

been presented (i.e., if there exist an obligation to affirmatively delete the preserved data).

3.5.5 Obligation of confidentiality

Article 16(3) provides that the preserved data must be kept confidential, and leaves it up to domestic law to define the necessary legislative measures to ensure this. The obligation to keep data confidential is motivated by two reasons: 1) the privacy of the person(s) involved, and (2) to avoid that the data are destroyed or tampered with. The dual obligations to keep the data safe and secure and to maintain confidentiality of the fact that the preservation measure has been undertaken helps to protect the privacy of the data subject or of other persons who may be mentioned or identified in that data.[63]

3.6 Article 17 – Expedited preservation and partial disclosure of traffic data

Article 17 establish the requirements for Member States to make sure that traffic data will be preserved and partially disclosed, whether one or more service providers are involved in the communication. The Article reads:

> *1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:*
>
> *a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and*
>
> *b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.*
>
> *2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.*

---

[63] Explanatory Report para 163

The purpose of the Article is to give law enforcement authorities a tool to determine the source and/ or the destination of the communication. This will enable the police to trace the origin of an offence, and follow the "electronic trail back to the person responsible through several service providers.

The Article gives no guidance on how this is to be done. The Explanatory Report states that it is up to "…domestic law to determine means that is consistent with its legal and economic system".[64] The infrastructure for Internet does not normally provide an automated mechanism for identifying the true source. Therefore, investigators will often need to contact individually each service provider in the chain, to determine the source of the prior connection.

3.6.1 Identifying different service providers

The Explanatory Report suggests three different methods how expedited preservation and –disclosure may be achieved when more than service provider is involved in the communication:

- Issue a separate order on each service provider
- Obtain one single order that apply to all service providers
- Require the service provider(s) to notify the next service provider in the chain

As for the first, a separate order on each service provider would be the traditional procedure for seeking disclosure of the data. The drawback is that it may be time-consuming.

[64] Explanatory Report para 168

One single order that applies to all service providers will be a lot faster, an important plus because the need to follow the track when it is "hot" and before data is deleted or altered.

The most controversial suggestion, however, is to obtain an order that involves the participation of service providers. A service provider, that somehow has been linked to a criminal offence, would be served with and order to notice the next service provider in the chain of the existence and terms of the preservation order. The second service provider would identify and notice the next, and so on.

The problem with the last alternative is that national laws are likely to require a judicial order to mandate preservation or disclosure of confidential data.[65] Identifying the next service provider in chain will most probably involve disclosure of confidential information, such as personal information and traffic data related to users and subscribers. Within the EU area, privacy laws give extensive provisions on how personal data are to be processed.[66] Such legislation does not apply to the area of crime control, but will have an effect in this matter when one (private) service provider reveals personal information of users to another (private) service provider.

In my opinion, the preferable way would be for the law enforcement authorities to ask for this information.

---

[65] In Norway, the Norwegian Post and Telecommunications Authority give such authorization. See also Rt. 1999 s. 1944 (access to traffic data).

[66] See section 5.3 below

3.7 "Competent authority"

3.7.1 Partial disclosure

Article 17(1) (b) of the Convention provides that the expedited disclosure of sufficient information to identify the service providers can be justified to a "competent authority"[67] while waiting for a judicial order to disclosure data to the law enforcement authorities. This implies, of course, that the "competent authority" has competence to evaluate what information that is relevant and sufficient in the particular case under investigation.

3.7.2 Production order

Article 18 provides instructions for Parties to enable their "competent authorities" to give orders of data preservation, while law enforcement authorities issue a search warrant. The implementation of such a "production order" will probably be beneficial to third party custodians of data, such as service providers, to relieve them of any contractual or non-contractual liability.[68]

3.7.3 Link to subscriber data

To be able to get data that are useful for law enforcement purposes, traffic data has to be possible to link to subscriber identity. The Explanatory Report explicitly states that the Article 18 should not be understood as to impose an obligation on service providers to keep record of their subscribers, and will not require service providers to ensure the correctness of such information.

---

[67] In UK, an "competent authority" could be any of the 1,039 public authorities authorised under the Regulation of Investigatory Powers Act 2000 – for which there is no comprehensive oversight in place

[68] Explanatory Report para 171

Thus, a service provider is not obliged to register identity information of so-called prepaid cards for mobile telephone services.[69] Nor is it obliged to verify the identity of the subscribers or to resist the use of pseudonyms by users of its services.[70] The proportionality principle will also provide some flexibility in relation to the application of the measure, for instance in many States to exclude its application in insubstantial cases.[71]

3.8 Mutual assistance regarding provisional measures

Articles 29 and 30 provides for a mechanism at the international level equivalent to that provided for in Articles 16 and 17 for use at the national level.[72] Preservation is a limited, provisional measure intended to take place much more rapidly than the traditional mutual assistance, which may take weeks or months. Article 29 specifies that preservation effected in response to a mutual assistance request "shall be for a period not less than 60 days in order to enable the requesting Party to submit a request for search or similar access, seizure or similar securing, or disclosure of data".[73] The reason is that traditional mutual assistance procedures are usually is time-consuming, and the provision ensures a minimum period of time for the requesting Party to issue a formal mutual assistance request seeking the disclosure of the data. Important to note, the Articles does not contain any guidance of the maximum allowed storage period. This could imply that the maximum period is 90 days in accordance with Articles 16 and 17, or that the question is left for national legislation.

---

[69] In Norway, e.g. the service provider Netcom estimates that they have approximately 300.000 users that are unknown, because any subscriber data has not been registered.

[70] Explanatory Report para 181

[71] Explanatory Report para 174

[72] Explanatory Report para 282

[73] Explanatory Report para 162

Where the requested Party believes that preservation will not ensure the availability of data, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed – Article 29(6).

According to Article 30 (2), disclosure of data may only be withheld if the request concerns an offence that the Party, to whom the request was made considers a political offence, or the execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. The Explanatory Report (para 291) states that the grounds for refusal are to be strictly limited, because this type of information is so crucial in identifying the perpetrators.[74]

3.9 Summary

In sum, this means that the Cybercrime Convention provides only for power to preserve data; pending subsequent disclosure of data to other legal power. This is limited to specific criminal investigations in a particular case, and presupposes that data already exist. The Convention does not require contracting Parties to collect or store data as a routine matter for purposes outside their normal business practice.

One of the primarily aims of the Convention is to achieve greater degree of harmonization of criminal laws of the Contracting Parties.[75] Since the Convention is drafted at a general level and leaves many of the details and safeguards up to national law, contracting Parties will have a significant leeway when implementing the Convention. This may actually hamper the harmonization and lead to less certainty in the area of crime laws.

---

[74] Article 26 enables a contracting party that possesses valuable information to forward it to another without prior request – "spontaneous information" – in certain situations. The article is derived from similar provisions in anti-corruption laws; see further Explanatory Report para 260-261.

[75] See the Preamble to the Convention and the Explanatory Report

The Convention aims at attracting the largest possible number of contracting Parties, as this will be essential to effectively fight cybercrime.

4 Data preservation vs. data retention

4.1 Is data preservation sufficient for law enforcement purposes?

A major concern for law enforcement authorities[76] is whether the preservation requirement will be sufficient to investigate and computer-related crime. There exist several reasons for this: First, data protection laws restricts the amount of data that can be stored, and require personal data to be deleted unless otherwise explicitly required by national laws. The principles of data protection laws prohibit service providers to keep personal data on the sole basis of potential further need expressed by law enforcement authorities.[77] Second, service providers tend to store less and less data, because of flat rate schemes or prepaid payment methods.[78] Third, those service providers that keep billing data rarely need to keep them for more than 3 months for business reasons. Some service providers even delete data after 24 hours. The term of the actual retention is often deemed to be to short to combat certain types of crimes.

---

[76] The following presentation is based on a subset of statements of UK law enforcement, available at http://www.apig.org.uk/lea.pdf and http://www.apc.org/english/rights/europe/eu/data_protection.html (accessed 25 July 2003), Inger Marie Sunde: "Convention on cybercrime", *Tidsskrift for strafferett* 1/2002, and Allitsch, p. 161 (on law enforcement views), as these probably represents opinions that are common in the law enforcement community.

[77] See further section 5.3 below

[78] The price charged for a communication is becoming less and less dependent on distance and destination, there is no longer any need to store traffic data for billing purposes

It takes, due to judicial difficulties, quite some time to discover the source of the attack. And, anonymous communication services[79] will prevent data from being available for law enforcement authorities.

All of the above may slow police work down, as valuable evidence may be destroyed. There is a fear that organized crime may exploit the opportunities of lack of such data as evidence, and take advantage of the weaknesses in the "trace route" to distance themselves from law enforcement. Traffic data can often be the only opportunity to trace criminals in a networked environment. It is therefore essential to ensure that relevant data exist to be accessed. From a police point of view, traffic data logs are necessary, and it is desirable that such logs are stored as long as they can be to any use in crime investigation. This is crucial for law enforcement, not only for safeguarding national security (i.e. against terrorism) but also to the detection of volume crime at the lower level.

4.2 Different concerns to be taken into account

Luc Beirens, Head of The Federal Computer Crime Unit of the Federal Police in Belgium, says that the destruction of traffic data "would have the same effect as wiping out all fingerprints and bloodstreams in the scene of a bloody murder before any police investigation could start".[80] At the other side, privacy interest groups[81] claim, "The traffic data of the whole population of the EU (and the countries joining) is to be held on record. It is a move from targeted surveillance to potentially universally surveillance"

---

[79] See section 5.4 below

[80] Statement made at the EU Forum on Cybercrime in Brussels; quoted by Allitsch, p. 161

[81] Statewatch 12 no 3 / 4 May-July 2002, see www.statewatch.org for more information (accessed 25 July 2003)

In other words, there are quite different interests at stake: 1) law enforcement authorities have stated that they consider the retention of a minimum of traffic data for a minimum period of time necessary to facilitate criminal investigations, [82] 2) privacy interest groups and data protection authorities fear that mandatory data retention will lead to excessive surveillance and potential misuse, and 3) the service providers fear that mandatory retention of traffic data will be unreasonably costly, in addition to hampering the development of the information society. Several industry associations have participated in the ongoing debate and made common statements.[83] This will be further dealt with in Chapter 8 below.

4.3 Mandatory retention of traffic data

Following the events of 11 September 2001, the law enforcement authorities increased the pressure on governments to adopt mandatory data retention requirements to fight terrorism. Several countries, such as e.g. Denmark (see section 7.1 below) have introduced such laws as a direct consequence of the terrorist attacks in New York and Washington.

---

[82] EU COM (2000) 890 final on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime, Brussels, 2 January 2001, available at http://europa.eu.int/ISPO/eif/internetpoliciessite/crime/crimecommEN.html (accessed 25 July 2003)

[83] See for example "Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes" of 4 June 2003 by ICC, UNICE, EICTA and INTUG, available at http://www.iccwbo.org/home/menu_electronic_business.asp or "Communications Data: Report of an Inquiry by the All Party Internet Group" of January 2003, available at www.apig.org.uk/APIGreport.pdf (accessed 25 July 2003)

The Belgian government drafted (and circulated for comment) in 2002 a Framework Decision on the retention of traffic data and access for the law enforcement authorities.[84]

The Draft Framework Decision was supposed to be a binding measure on all EU member states. The reasoning was that effective investigation and surveillance would break down if not all countries allow data retention and subsequent access to the data by law enforcement authorities. The Draft Framework Decision proposed that data should be retained for 12 to 24 months.[85] The police would still need a judicial order for access to the data. The Draft Framework Decision defined traffic data as "all data processed which relate to the routing of a communication by an electronic communications network" (Article 1(a)). The definition is very broad, as it would apply to all data in relation to land and mobile telephones and Internet connections. No necessity criterion is included in the definition. The Decision would apply to criminal investigation in general, and not limited to terrorism or other serious crimes.

The Draft Framework Decision is not an official document, but was leaked to Statewatch, that published it along with much critical commentary.

4.4 Opinion of the European Data Protection Commissioners

The European Data Protection Commissioners has warned about the possible lack of legitimacy and legality of mandatory data retention for law enforcement purposes. Traffic data reveal enough information to analyze the personal and social relationship

---

[84] "Surveillance of Communications: data retention to be 'compulsory' for 12-24 months", Statewatch analysis no 11, May 2002, full text of the Framework Decision is available at www.statewatch.org/neww/2002/aug/05datafd1.htm (accessed 25 July 2003)

[85] A substantial longer period of time than the maximum of 90 days in Article 16 of the Cybercrime Convention, cf. Peter Blume, "Overvågning af og i cyberspace", *Fra rådet til tinget,* No. 166 (2002)

and the use of media of a given person. Aggregation of such information over a longer term allows the compilation of a profile.[86] The Commissioners emphasize that such retention will be an improper invasion of the fundamental rights guaranteed to individuals be Article 8 of ECHR. Retention of traffic data for purposes of law enforcement should meet strict conditions, i.e. only on a case-by-case basis for a limited period and when necessary, appropriate and proportionate in a democratic society. At the International Conference in Cardiff (9-11 September 2002), [87] the Commissioners made a common statement on mandatory data retention:

> *"Where traffic data are to be retained in specific cases, there must therefore be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law, in a way that provides sufficient safeguards against unlawful access and other abuse. Systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case."*

The Commissioners were also worried about the costs involved, and noted the absence of any similar measures in the United States - a telling observation since the idea stems from post 11 September 2001 "terrorism investigation requirements".

4.5 Privacy issues

The purpose of Article 15 of the Cybercrime Convention is to balance data preservation requirements with the protection of human rights and liberties. However, data retention requirements are not addresses in the Convention. Data retention and subsequent access to that data is a complex topic.

---

[86] Allitsch, p. 164

[87] Statement of the European Data Protection Commissioners 11 September 2002, published at the website of Foundation for Information Policy Research (FIPR), available at http://www.fipr.org/press/020911DataCommissioners.html (accessed 25 July 2003)

The debate recently has therefore been whether the requirements of data retention are compatible with privacy laws. Privacy spokespersons and the police tend to have very different views on how the law should be. As quoted above, the European Data Protection Commissioners find that data retention by service providers would be an improper invasion of the fundamental rights guaranteed to individuals by the European Convention on Human Rights.

The Global Internet Liberty Campaign (GILC), a coalition of 60 liberties groups, organized in 2002 a campaign against data retention.[88] More than 16,000 individuals from 73 countries endorsed it in a matter of days. In an open letter to Pat Cox, President of the European Parliament 22 May 2002 it is opined that: "While the fight against terrorism is a legitimate purpose, we do not believe it can justify actions that undermine one of the most fundamental rights of democratic states.[..] New retention requirements […] will create new risks to personal privacy, political freedom, freedom of speech, and public safety.[…]. Wide data retention powers for law enforcement authorities, especially if they were used on a routine basis and on a large part of the population, could have disastrous consequences for the most sensitive and confidential types of personal data." If such a general power were enacted into law, it would amount, for many privacy law experts, to a blatant violation of the fundamental rights of presumption of innocence, privacy, freedom of expression, and secrecy of communications.

The most central privacy related issues with regards to data preservation and data retention will be highlighted below.

---

[88] April-May 2002 Campaign against data retention: Open letter to Pat Cox, President of the European Parliament 22 May 2002. Available at http://www.epic.org/privacy/intl/data_retention.html#humanrights (accessed 25 July 2003)

5 Relation to privacy laws

5.1 The right to privacy

To my knowledge, the term "privacy" is not clearly defined in any data protection law,[89] but judicial theory has traditionally defined the concept in different ways. [90] Definitions of privacy vary widely according to to context and environment. Privacy is seen as an important right in a democratic society, to encourage individuals to participate in political and social life and thereby ensure a diversity of opinion and lifestyles.[91] It has also been used as a protection for the individual against potential misuse and excessive control by public administration.[92]

---

[89] Article 1(1) of Directive 95/46/EC instructs the member states to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy…". The object of CoE Convention on data protection[89] is formulated in similar ways. Recital 10 of the Directive 95/46/EC elaborates the concept of privacy as that "which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law".

[90] See further Bygrave, *Data Protection Law – Approaching Its Rationale, Logic and Limits*, p. 125, and Electronic Privacy Information Centre, "Privacy and Human Rights 2002 – An International Survey of Privacy Laws and Developments" (Washington DC, 2002), available at www.privacy.org/pi/survey/phr2002/phr2002-part1.pdf (accessed 25 July 2003)

[91] Bygrave, *Data Protection Law – Approaching Its Rationale, Logic and Limits,* p 135

[92] See section 5.2.2 below

5.2 Human Rights Conventions[93]

5.2.1 General

The right to privacy is set out in several human rights conventions, such as the Universal Declaration of Human Rights (UDHR) of 1948, the International Covenant on Civil and Political Rights (ICCPR) of 1966 and the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) of 1950.[94]

5.2.2 Article 8 of ECHR

Article 8 of ECHR protects the individual against arbitrary interference by public authorities in his private or family life, including his correspondence.[95] Exemptions are made if the interference is "…in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention or disorder of crime….", Article 8(2).

Much of the case law of the European Court of Human Rights (EctHR) pursuant to Article 8 concerns surveillance activities by police or state agencies. Leading cases are *Klass and Others v Germany*[96] and *Malone v. United Kingdom*.[97] It may be concluded

---

[93] See further Bygrave, "Data protection pursuant to the right of privacy in Human Rights Treaties" *International Journal of Law and Information Technology*, 1998, Volume 6, pp. 247-284

[94] See also The American Declaration of the Rights and Duties of Man (ADRDM) of 1948, the American Convention on Human Rights (ACHR) of 1969. The African Charter on Human and People's Rights (ACHPR) of 1981 is the only convention without an express protection for privacy.

[95] Cf. Art 12 of UDHR, Art 17 of the ICCPR, art V of the ADRDM and Art 11 of the ACHR

[96] ECtHR Judgment in the case of Klass and others v. Germany, A28, 06/09/1978, as referred to in Bygrave, "Data Protection Pursuant to the Right to Privacy in human Rights Treaties" p. 9

[97] ECtHR Judgment in the case of Malone v. United Kingdom, A82, 02/08/1984, as referred to in Bygrave, "Data Protection Pursuant to the Right to Privacy in human Rights Treaties" p. 9

from case law that interception of a person's communication constitutes an interference with the person's right under Art 8(1), but the interference may be justified under Article 8(2) if three cumulative conditions are justified: a) the interference must be in accordance with the law, b) it must be necessary in a democratic society; c) and in the interest of national security or public safety, for the purposes specified in Art 8(2).

Data retention requirements for crime prevention purposes would involve the routine collection and storage of traffic data on a large part of the population, by private entities. Since today's traffic data (cf. Annex I) have the potential to generate extensive information of individuals, it has been argued that the retention of traffic data in any case should be considered as interference with the private life in the sense of Article 8 ECHR.[98]

However, any legislative measure at national level that may provide for the retention of traffic data for law enforcement purposes would need to fulfill the conditions as listed above. In this context it can be assumed that condition c) above is fulfilled, i.e. for the purpose of crime prevention.[99] The condition of "in accordance with the law" has been interpreted to not necessarily require any legislative authority; however the authority must though satisfy typical "rule-of-law" principles like forseeability, clarity and non-arbitrariness.[100]

---

[98] Allitsch, p. 166

[99] However, the measure implemented to prevent crime must be proportional to the aim pursued. I.e., if there exist less intrusive means, these will prevail.

[100] See further Bygrave, "Data protection pursuant to the right of privacy in Human Rights Treaties", pp. 247-284

Necessity in a democratic society "corresponds to a pressing social need" and is "proportionate to the legitimate aim pursued".[101] These phrases are very vague, and their meaning would probably change during time and within different cultures. However, the proportionality assessment varies according to 1) the gravity of the interference, 2) the sensitivity of the information and 3) the safeguards implemented. "States may not…, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate… the danger (is that) of undermining or even destroying democracy on the ground of defending it", see *Klass* (A28).

Applied to data retention, the "necessity" criteria and Article 8 case law has been interpreted to imply that the public authorities may only have access to traffic data on a case-by case basis, and never proactively as a general rule.[102]

5.3 Data Protection laws

5.3.1 General

The right to privacy is pursued in data protection laws. One of the most important legal instruments is the Council of Europe Convention for the protection of individuals with regard to processing of personal data.[103] It is the sole international, legally binding treaty dealing with data protection.[104]

---

[101] See ECtHR Judgment in the case of Leander (Fn 29) para 58, available at http://www.menneskeret.dk/menneskeretieuropa/konventionen/baggrund/domme/ref00000104/ (accessed 25 July 2003)

[102] Allitsch p. 166

[103] *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, Strasbourg 28 January 1981

[104] Bygrave, *Data Protection Law- Approaching Its Rationale, Logic and Limit,* p. 32

Within EU, Directive 95/46/EC[105] provides comprehensive regulations for the processing for personal data. Also worth mentioning is the OECD Guidelines[106] governing the protection of privacy and transborder flows of personal data, and the UN Guidelines[107] concerning computerized personal data files. They are not legally binding (cf. the word "guidelines") but serve as models and are highly influential in non-European jurisdictions.[108]

5.3.2 Data protection principles[109]

The above-mentioned instruments establish certain principles on how processing of personal data are to be carried out. Some of the principles are particular relevant in the context of data retention:

5.3.2.1 Principle of fair and lawful processing

Personal data undergoing automatic processing shall be "obtained and processed fairly and lawfully", CoE Convention Article 5(a), cf. Directive 95/46/EC Art 6(1)(a), UN Guidelines principle 1 and OECD Guidelines para 8.

---

[105] See further section 5.3.3 below

[106] *Organization for Economic Co-operation and Development (OECD) Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data*, 23 September 1980

[107] *United Nations (UN) Guidelines concerning computerized personal data files*, 14 December 1990,

[108] E.g. Japan and North-America, cf. Bygrave

[109] For further elaboration of data protection principles, see Bygrave, *Data Protection Law - Approaching Its Rationale, Logic and Limits.* Bygrave lists the core principles of data protection laws as: Fair and lawful processing, Minimality, Purpose specification, Information Quality, Data subject participation and control, Disclosure limitation, Information security and Sensitivity.

Applied to data retention, this means that the laws need to specify clearly what types of data that are allowed to be retained, for how long and by whom.

5.3.2.2 Principle of Minimality

Personal data must be "…adequate, relevant and not excessive in relation to the purposes for which they are collected" (Article 6(1)(c) of the Data Protection Directive). This is often referred to as the principle of minimality. Articles 7 and 8 of the Directive also promote minimality of data collected and processed, and similar provisions is found in CoE Convention on data protection Article 5(d), OECD Guidelines para 8 and UN Guidelines principle 2. According to sector-specific regulation within telecommunications, traffic data is only allowed to be stored for business purposes, such as billing and maintenance (see 5.3.3 below). The principle is recognized in the promotion of technical standards that allows for a minimality of data to be collected, (see 5.4 below).

5.3.2.3 Principle of Purpose Specification

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (see Directive 95/46/EC, Article 6(b)). Similar provisions exist in CoE Convention Art 5(6), OECD Guidelines para 9 and UN Guidelines principle 3. When the service providers collect subscriber information for billing purposes, a disclosure to law enforcement authorities in crime investigations will consequently involve a repurposing of the use of the data.[110] The data must not be kept in a form that permits identification after they no longer are necessary for the purposes the data where collected (Article 6(1)(e)).

---

[110] However, the data protection directive does not apply to the areas of criminal law, see Article 3(2) cf. recital 13.

This principle is also present in CoE Convention Article 5(e) and as a "use limitation" principle in OECD Guidelines. Article 6(1) of Directive 2002/58/EC states that traffic data must be deleted when they are no longer needed for billing.

5.3.3 EU Directives on Privacy

5.3.3.1 General

In the European Union, Directive 95/46/EC provides for the harmonization of the national legislation of the member states required to ensure an equivalent level of protection of fundamental rights and freedoms and in particular the right to privacy with respect to processing of personal data and to ensure the free movement of such data within the Community.[111]

In 1997, the European Union supplemented the general Directive 95/56/EC with the more specific Directive 97/66/EC in the telecommunication sector. This directive will by the end of 2003[112] be replaced by Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic sector. The new directive is supposed to strengthen privacy rights for individuals by extending the protections that where already in place for telecommunications to a broader, more technology-neutral category of "electronic communications".[113]

---

[111] Recital 10 of Directive 95/46/EC

[112] In Norway, the directive will be implemented by the new Ekom Act

[113] Recital 4 of Directive 2002/58/EC

The Explanatory Report to the Cybercrime Convention discusses the relation to the data protection directives in para 154:

> *"These directives establish the obligation to delete data as soon as its storage is no longer necessary. However, Member States may adopt legislation to provide for exemptions when necessary for the purpose of the prevention, investigation or prosecution of criminal offences.* ***These directives do not prevent Member States of the European Union from establishing powers and procedures under their domestic law to preserve specified data for specified investigations****"* (emphasis added).

As discussed above (section 3.4.1), the Cybercrime Convention aims for a minimum level of legal protection and procedures recognized in national laws (e.g. data preservation), and do not contain any prohibition for countries to impose additional requirements under their legal system (e.g. data retention). The Explanatory Report does not comment on whether the privacy directives would prevent the member states to require systematically retention of traffic data.

5.3.3.2 Obligation to delete data

Directive 97/66/EC and Directive 2002/58/EC establish the obligation to delete certain types of data, such as personal data, if there is no longer a business purpose for the retention of the data.

Article 6 (1) of Directive 97/66/EC reads:

> *"Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/ or publicly available telecommunication service* ***must be*** *erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2,3 and 4."* (Emphasis added)

The Article requires that the data should be deleted once it is no longer required for the purpose for which it was collected. Article 14(1) allows member states to restrict the scope of obligations provided for in Article 6 when such a restriction constitutes a

necessary measure to safeguard national security and for the prevention, investigation and prosecutions of criminal offences as referred to in Article 13(1) of Directive 95/46/EC.

Article 6 of Directive 2002/58/EC carries on the obligation to delete data from Directive 97/66/EC. The directive was supposed to be an uncontroversial update of the existing directive, but following the events of 11 September 2001 the question of mandatory data retention came up. Data retention was subject of a lengthy debate, but was left to the member states to decide after certain safeguards were fulfilled.

Recital 26 provides that data relating to subscribers may only be stored "...to the extent necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time". This implies that data should be stored for a limited period only and not routinely held for extensive periods.

Article 6(1) of Directive 2002/58/EC reads:

> *"Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public communications network or publicly available electronic communication service* ***must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication*** *without prejudice to the provisions of paragraphs 2,3 and 5 of this Article and* ***Article 15(1)****."* (Emphasis added)

Article 15(1) expressly provides that a member state may derogate from Article 6 "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard… the prevention, investigation, defection and prosecution of criminal offences or of unauthorized use of the electronic communications system…"[114]

[114] Cf. Article 13 of Directive 95/46/EC

This allows member states to restrict the scope of the obligation to delete data by introducing new laws mandating data retention. The data that can be retained includes catalogues of web sites visited, records of e-mail recipients, lists of telephone numbers dialed ("traffic data"), and the geographical location of the user by fixed or mobile phones ("location data") (Art 2(b) and (c) of Dir. 2002/58/EC).

5.3.3.3 Confidentiality of the communication

In European Union, there is a general principle of confidentiality of communications (and related traffic data). Interceptions are illegal, unless law when necessary in specific cases, authorizes them for limited purposes. This follows from Article 8 of the European Convention of Human Rights, and the above-mentioned data protection directives. Illegal interception is established as an offence under Article 3 in the Cybercrime Convention, and applies in principle to all forms of data transfer, whether by telephone, fax, e-mail or file transfer.[115] It represents the same violation of privacy of communications as traditional tapping and recording of oral telephone conversation between persons. Article 5 of Directives 97/66/EC and 2002/58/EC establishes a duty for member states to ensure the confidentiality of communication, and prohibit "listening, tapping, **storage** or other kinds of interception…." (emphasis added) except when legally authorized. Since today's communication data may contain indicators of content, i.e. web sites visited etc., mandatory data retention could in some situations be a threat to the confidentiality of communication.

[115] Explanatory Report para 51

5.3.4 Summary

In sum, the data protection directives establish a duty to delete data no longer needed for business purposes. However, the directives do not apply in the field of crime law, and member states may therefore introduce new laws of mandatory data retention.

However, any legislative measure at national level that may provide for the retention of traffic data for law enforcement purposes need to fulfill certain conditions: the proposed measures need to be appropriate, necessary and proportionate, as required by Community law and international law, including Directive 97/66/EC and 95/46/EC, the European Convention for the Protection of Human Rights of 4 November 1950 and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 28 January 1981. This is particularly relevant for measures that would involve the routine retention of data on a large part of the population.[116]

5.4 Anonymisation services

Several initiatives have been introduced to promote privacy and anonymity in cyberspace. One initiative is the development of privacy enhancing technologies (PETs), which promote technical standards that allows for a minimality of data to be collected.[117] This has fundament in several EU directives:

The Universal Services Directive (Directive 2002/22/EC) provides in Article 10, cf. Annex I part A (c) that Member States shall provide mechanisms for pre-payment[118]

---

[116] EU COM (2000) 890 final: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime

[117] Examples of PETs are encryption, pre-paid phone cards, anonymisation software etc.

[118] Examples of pre-payment methods are phone-cards, flat-rate subscriptions, phone box etc.

methods for telephone services. With such a requirement, there is no business reason for service provider to keep subscriber data or traffic data for billing purposes. That means, when law enforcement authorities need traffic data to investigate a crime, no such data exists. Even if the directive specifies this applies to "telephone" services, the service providers already offer pre-payment methods or flat rate services for communication in general. Broadband connections frequently use this billing method.

The German Teleservices Data Protection Act of 22 July, 1997[119] explicitly states in Section 4(6) that the provider shall make it possible for the user to utilize and pay for teleservices anonymously or under a pseudonym it this is technically possible and can be accomplished at reasonable effort. The user shall be informed of this possibility.

Recital 30 of the Directive 2002/58/EC includes similar statements: System for the provision of electronic communication networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users. Recital 33 of the Directive follows up with "…in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example calling cards and facilities for payment by credit cards."

---

[119] Act of the Protection of Personal Data Used in Teleservices (Teleservices Data Protection Act – *Teledienstedatenschutzgesetz TDDSG*) of 22 July, 1997, amended last by Article 3 of the bill on legal framework conditions for electronic commerce

There exist several services on the Internet that offers anonymous surfing,[120] by use of proxy servers[121] or software that promotes anonymity.[122] The deployment of such services is suitable for those worried about their privacy, and also for criminals that do not want to be traced by the police. Law enforcement experts have expressed concern that anonymity may result in non-accountability and could seriously impede the possibility to catch certain criminals.

6 Relation to the E-Commerce Directive

6.1 General

The development of the information society is believed to be a key factor to ensure economic and social growth in Europe. It is a policy goal to take full advantage of e-commerce to achieve full impact of the internal market and free movements of goods, people, services and capital.[123] However, realizing that this goal may be hampered by divergences in legislation and from legal uncertainty as to which national rules apply to

---

[120] Examples of websites that offers anonymous search are www.safeproxy.org and www.jupe.dk (accessed 25 July 2003)

[121] A proxy server is a kind of buffer between the computer and the Internet resources the user are accessing (e.g. web sites). The data the user request comes to the proxy first, and only then transfers the data to the user. If a proxy sits between the user and the Internet all of the users appear to come from one computer. In these cases, users can only be traced as far as the proxy unless additional information is known.

[122] Anonymisation software are available from 30$ at www.anonymizer.com (accessed 25 July 2003)

[123] Recitals 1-5 of Directive 2000/31/EC

such services, the European Parliament and the Council of Europe has passed a Directive on E-commerce (Directive 2000/31/EC).

It has been discussed to what extent service providers should be liable for illegal content and criminal offences committed through their servers and networks. It was not desirable to put to heavy restrictions and liability on the service providers as this may hamper the development of the information society. If the service providers are not willing to be exposed to such risks, the information society will suffer. The directive therefore provides certain "safe harbors" from liability for service providers.

A study on the legal issues relevant to combating criminal activities perpetrated through electronic communications,[124] points at the fact that systematic storage of communications content by a service provider has potential contractual liability implications towards subscribers. The potential liability of service providers arising from data retention practices should be limited,[125] and any data retention measure therefore needs to be well founded in law to avoid contractual liability.

Two of the Articles are particularly interesting in relation to the duty to preserve data under the Cybercrime Convention, and will be discussed below.

6.2 Liability of intermediary service providers

Directive 2000/31/EC provides exemptions from liability where the service providers only performs certain necessary acts in the communications process; mere conduit (Article 12), caching (Article 13) and hosting (Article 14). The service providers have

---

[124] The Computer Related Crime Research Unit, "Study on the legal issues relevant to combating criminal activities perpetrated through electronic communications – Final Report" (London, 2000), available at http://europa.eu.int/ISPO/eif/internetpoliciessite/crime/study2000/cover.html (accessed 25 July 2003)

[125] G8 Report

no general obligation to monitor content or traffic (Article 15). The exceptions will only apply when the service provider acts as an intermediary in the communication process.

6.2.1 Article 14 – Hosting

Article 14 exempts service providers from liability if they does not have actual knowledge or are aware of facts and circumstances of illegal content or activities. The service provider has to act quickly to remove the information or disable access to it upon obtaining such knowledge[126] to be able to escape liability.

That means, if any electronic evidence is needed at a later stage (cf. Articles 16 and 17 of the Cybercrime Convention), the information may already be deleted of the service provider to avoid liability.

However, recital 46 of Directive 2000/31/EC gives the Member states the opportunity to "…establish specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information". Member states may therefore provide at national level that such data are preserved for a later investigation.[127]

6.2.2 Article 15 – No general obligation to monitor

Article 15 states that service providers shall have no obligation to monitor information they transmit or store, or to actively seek facts or circumstances indicating illegal activity.[128] The service providers are not obliged to investigate illegal activity

---

[126] What constitutes actual "knowledge" may be subject for discussion, but will not be pursued here

[127] In EU, a procedure like "notice-and-takedown" like in the U.S. Digital Millennium Copyright Act (DMCA) was rejected of several reasons. This will not be further dealt with here.

[128] This harmonizes with the Cybercrime Convention's Explanatory Report that applies Article 16 on data that "already exits", i.e. no obligation for the service providers to implement routines above what that they use in their normal business practices.

themselves, but leave this up to the law enforcement authorities. However, recital 48 of the directive establishes that Member States may impose a "duty of care, which can reasonably be expected of them and which is specified by national law, in order to detect and prevent certain types of illegal activities". The duty of care is expected to consist of implementing and operating filtering and control mechanisms.[129]

Article 15 (2) establishes that Member States may require that information society providers promptly inform the competent public authorities of alleged illegal activities undertaken and at their request provide information that enables the identification of users. This may be contradictory compared to the provisions of the data protection directives: Recital 14 of Directive 2000/31/EC states that Directive 95/46/EC and Directive 97/66/EC are fully applicable to information society services, and that implementation of Directive 2000/31/EC should be made in full compliance with the principles relating to the protection of personal data. Recital 15 reaffirms that the confidentiality of communications is guaranteed by Article 5 of Directive 97/66/EC, and provides that Member States must prohibit any kind of interception or surveillance of communications by others than the senders and receivers, except when legally authorized.

---

[129] Rosa Julia-Barcelo, "Liability for on-line intermediaries: comparing EU and US legal frameworks" in Unipub AS', *Required reading Part I, E-commerce law, Masters of Law* (Oslo: Kopinor, 2003) p. 252. Barcelo ask whether this recital mean that Member States are entitled to impose monitoring obligations on service providers, but concludes that taking into account the existence of Article 15.1 and the fact that the monitoring statements are included in a recital rather than in the main text, it seems rather likely that the service providers will not be obliged to monitor content on a general basis. Service providers may also claim that given the vast amount of material placed on its servers, it is technically impossible for it to monitor the content of its servers.

6.3 Summary

A potential conflict exists in the Cybercrime Convention's requirements of expedited data preservation, and the obligations of "expeditiously" removing illegal content under Directive 2000/31/EC. Further guidance on how these provisions are to be understood would be desirable. Divergence in legislation is a potential obstacle within the internal market for the growth of e-commerce; not to forget the hampering effect for cross-border investigation of computer crimes.

7 Current Practice

7.1 Europe

According to a survey by the European Council on traffic data retention,[130] a majority of EU governments have or intend to introduce an obligation for the retention of traffic data, in case the information became of might prove useful in police or security service investigations. The norm for the period of data retention would appear to be 12 months, although Ireland is way put ahead with 3 years.

Examples of countries that have already introduced such legislation, is e.g. Denmark and the UK. In Denmark, The Danish Administration of Justice Act was amended by Act No 378 of 6 June 2002 (the Anti-Terrorism Act of the Ministry of Justice). Section 786 has been amended so that communications providers have to retain data for 12 months. The UK Government introduced the Anti-Terrorism Crime and Security Act in

[130] Answers to questionnaire on traffic data retention, by Council of Europe 20 November 2002, available http://www.effi.org/sananvapaus/eu-2002-11-20.html (accessed 25 July 2003)

December 2001.[131] The government had hoped to persuade UK service providers to introduce these measures voluntarily, but the service providers remained unconvinced by the government's arguments and concerned about costs.[132]

The survey shows that governments across Europe are taking a similar line on data retention. Of the governments surveyed, Greece, Ireland, Italy, Luxembourg, Spain, Portugal, and Sweden support the idea of a European instrument, with Belgium also backing the proposals. Finland supports data retention, proposing to set a two years period for mandatory data retention, while France underlines that data retention is now "authorized" after its adoption of Directive 2002/58/EC. The only countries expressing reservations are Germany and Austria. German authorities say that they need proof that the proposed European instrument is compatible with German constitutional law.

7.2 USA

The US Government seems to have favored a move towards a preservation regime instead for retention requirements.[133] The reasoning has been that preserving data on an individual and identifiable suspect rather than historical data on all users offers at more balanced and proportionate solution. Law enforcement is provided with the evidence it needs without unduly impinging on citizens' rights or imposing unnecessary costs on service providers. In addition, the preservation approach preserves the important checks-and-balance system of judicial oversight of law enforcement activities. Rather

---

[131] Anti-Terrorsim, Crime and Security Act 2001, available at http://www.hmso.gov.uk/acts/acts2001/20010024.htm (accessed 25 July 2003)

[132] AGIP- Submission on behalf of UK Law Enforcement, available at http://www.apig.org.uk/lea.pdf (accessed 25 July 2003)

[133] See, 18. U.S.C. 2703, available on http://www.usdoj.gov/criminal/cybercrime/usc2703.htm, (accessed 25 July 2003)

than assuming everyone is possibly guilty, law enforcement is only able to obtain information based on specific evidence (suspicion) that a crime may have been committed. The government has in September 2002 launched a National Strategy to Secure Cyberspace,[134] which contains 5 national priorities including a National Cyberspace Security Response system that are planned to improve response to cyber incidents and reduce potential damages from such events.

8 Discussion topics

8.1 Privacy or security – a policy dilemma

Mandatory data retention is currently a dilemma for governments and policy makers. On the one hand, protection of privacy is essential if the right to anonymity and freedom of expression are to be maintained online. On the other hand, the right to privacy may cause security risks if the police are left without traces of criminal behavior. If there is given a right to anonymity for privacy reasons, this will also apply to criminals and thereby shield them from investigation and prosecution.

Protection of privacy has been a key policy objective in the European Union.[135] However, privacy is not an absolute right. The needs of the society as a whole must prevail. Independent of the individual's right to privacy, the question that must be

[134] National Strategy to Secure Cyberspace, available at http://www.whitehouse.gov/pcipb/ (accessed 25 July 2003)

[135] The European Parliament is sensitive to privacy issues and has generally taken a stance in favor of strong protection of personal data, cf. EU Forum on Cybercrime

discussed is whether it is desirable to have a society that keeps all its citizens under systematic surveillance.

Mandatory data retention could lead to a high degree of surveillance, as all citizens' private communication will be kept and stored for years. [136] There exist a certain fear that supply creates demand. As soon as comprehensive databases of the public's communication or activities exist, the pressure to use them for purposes beyond those for which they were chartered will increase. The unknown effects and potential for misuse is worrisome. If particular patterns of behavior were highly correlated to criminal behavior then it might become possible for "fishing expeditions" to detect these patterns to be seen a proportionate action.[137]

Thus, law enforcement authorities claim that communications data is becoming increasingly important to provide evidence to establish innocence. If such data is not available as evidence for prosecution or defense, this could lead to a miscarriage of justice. According to law enforcement authorities, this provides the overriding justification for longer-term retention.

A phrase sometimes used is "only the guilty have anything to fear". But critics point at the fact that it is not only law enforcement authorities or government that may pose a

---

[136] See, for example, Denise T. Rice: "2001: A Cyberspace Odyssey through U.S. and EU Internet Jurisdiction", PLI's Fifth Annual Internet Law Institute, San Fransiciso, July 2001: All 30 of the ISPs in Saudi Arabia are linked to a ground floor room at the Riyadh Internet entranceway where all of the country' web activity is stored in massive cache files and screened. Residents can circumvent government controls by connecting to the Web through foreign-based servers and through satellite phones or by using the file transfer protocol, but those methods require either money or some computer expertise.

[137] AGIP Report, quotation of Dr. Pounder, p. 8

threat to privacy: Traffic data are collected and stored by private service providers, with no prior authorization.[138]

It is very difficult to conclude what the better solution to the dilemma would be. The impact of any measure must be carefully analyzed and compared with the effectiveness of such a measure in the fight against cybercrime. Adequate security of any retained traffic data would have to be ensured.[139]

In my opinion, I personally would tend to favor a secure cyberspace even if this involves some sort of registration or data retention. I think this will be the only way to fight cybercrime, not necessary serious crime such as terrorism etc., but the lower level crime such as e.g. credit card fraud and child pornography. However, the dangers of an unwanted surveillance and control must not be neglected, and any measure should be subject for an extensive, public debate before it is introduced.

8.2 What data are required?

Important questions that need to be discussed are; what type of data should be retained for what reasons, for how long, and by whom?

Privacy interest is generally considered to be less with respect to the collection of traffic data than interception of content data. Traffic data about time, duration and size of communication reveals little information of personal interests. However, a stronger privacy issue may exist in regard to data about the source or destination of a communication (e.g. visited websites). This means that mandatory data retention

---

[138] See, Peter Blume, "Overvågning af og i cyberspace", *Fra rådet til tinget,* No. 166 (2002). Blume suggests that if data retention becomes mandatory, it might be appropriate to consider a further registration and approval of service providers.

[139] EU Forum on Cybercrime

requirements should only be applied to traffic data (and not content data). However, the distinctions between traffic- and content data are increasingly blurred, as discussed in 2.7, and it is increasingly difficult to strictly separate the two concepts of data.

There is a need to reach a common consensus for what purposes and to what extent particular types of traffic data may be generated, collected, stored, and for what purposes they might be further used. Further guidance and legislation on the issue would be desirable.

8.2.1 A new definition of traffic data

Important to note, the "traffic data" definition in Article 1(d) of the Cybercrime Convention does not contain any "necessity" criteria. The definition also differs from the definition of "traffic data" in Directive 2002/58/EC, Article 2(b). Given the wide (and different) definitions of traffic data, I think a new definition of traffic data – narrow and precise – is necessary. If not, there will probably be much uncertainty attached to what data are allowed, or required, to process and store. A new definition should be restricted to what data is necessary for the purposes for why they are collected, and the level of sensitivity of the data. This way, the distinction between traffic-, content- and location data could perhaps be avoided. If possible, effort should be made to define the necessary data and measures that do not involve overlapping storage of data, or the storage of excessive data.

8.2.2 Is there a need for a common measure throughout Europe?

If data retention practices are left to national laws, or service providers on a voluntarily basis, the risk is significant divergence between member states. The differing retention practices and access provisions could make police work more difficult. A survey conducted by the Council of Europe (see section 7.1 above) shows that a majority of governments within EU is supportive of a proposal of mandatory data retention and a

common legal structure. However, the law enforcement authorities point out that they can not wait for this to happen, and urges progress in national legislation in the meantime.[140]

8.3 Practical problems

8.3.1 Costs

There exists very little material on what the actual costs involved in data retention are. Questions still unanswered are; what are exactly the costs of mandatory data retention, what part of the process is most costly, who should bear the cost etc. Several figures have been presented, that varies significantly. [141] The government's estimates are far below what the industry itself suggests. A survey conducted by the All Party Internet Group[142] shows that this is due to the fact that the first mentioned take accounts of the cost of an access request, while the latter calculates the cost of storage, maintenance and accessibility of data.

---

[140] Several cases have been used for justifying the need for this, see e.g. "Communications Data: Report of an Inquiry by the All Party Internet Group" of January 2003, available at www.apig.org.uk/APIGreport.pdf (accessed 25 July 2003)

[141] See, e.g. Allitsch (p. 163) or All Party Internet Group (AGIP), "Communications Data – Report of an Inquiry by the All Party Internet Group" (p. 22): AOL, a large ISP operating at a global level, reported to AGIP that they processed 392 million user sessions a day, sending 597 million emails end estimated they would spend $40 million setting up a system and $14 million per annum running it. THUS plc estimated that within their business they could, at the upper end of what might be rquired, be looking at a five or six million pound project. When one considers the size of the rest of the ISP industry, let alone the fixed line and mobile telephone companies, the sums well in excess of £100 million might well turn out out to be necessary. All figures must bee seen as rought estimates.

[142] All Party Internet Group (AGIP), "Communications Data – Report of an Inquiry by the All Party Internet Group", p. 22

Some confusion arises because of doubt about exactly what must be stored for how long.[143] If service providers keep data for 3-6 months anyway, would it be substantially more cumbersome or expensive to keep data for 12 or 24 months? What about 10 years?[144] To my knowledge, no affirmative or common agreed answers exist.

Mandatory retention of traffic data for periods longer than business requires do not only magnifies costs, but also poses significant privacy and security risks by creating enormous pools of stored data, increasing the risk of illegal access to and misuse of this data. The data protection authorities will not have the capacity to effectively supervise the processing of personal data in such volumes.[145] Governments and service providers would need to develop appropriate security measures, at additional cost. [146]

The Common Industry Statement[147] opines that governments should bear the costs; "Requiring law enforcement authorities to bear the cost of access requests to the traffic data, they argue, will help to ensure that only strictly necessary requests for data are made, and will reduce public concern regarding the privacy implications of data storage. These safeguards will help ensure that the goals of the use of stored data are limited to what is in the public interest." [148]

---

[143] Ibid.

[144] The latter could probably run into some technical questions, because data is not only to be stored, but should be readable after 10 years as well. This may cause problems because of e.g. new storage mediums and new software.

[145] Allitsch, p. 164

[146] Common Industry Statement, p. 8

[147] Common Industry Statement, p. 3

[148] Common Industry Statement, p. 8

Additional costs of data retention could be identified on the basis of data storage, security measures, request compliance and staff costs. [149] If the service providers are to bear this cost as a "cost of doing business" the cost will eventually be allocated to subscribers and may hamper the development of the Information Society. In addition, if everyone who is engaged in providing communication services is required to retain data, there will be a considerable overlap in storage and considerable unnecessary expense. In many cases, more than one provider may be required to save the same traffic data, e.g., an Internet Service Provider and an email provider. As crime detection is considered to be in the interest of the public and consequently a common good, it is considered that there is no justification for the cost being borne by the industry.

In my opinion, further research on the different cost elements and cost-benefit analyses is urgently needed, and should be carried out by joint efforts of governments and the industry. This should be done as soon as possible, and before any further legislation is introduced on the same issue.

8.3.2 Technical requirements

Significant concerns have been raised about the possible imposition of data retention requirements in respect of data not currently recorded in the normal course of the service provider's business. The criticism against requirements of data retention are that the governments and law enforcement authorities often lacks the necessary in-depth technological knowledge of how retention and storage are carried out. The volume of data involved is also likely to be considerable and expanding at an exponential rate. Given the mass of data useful to retain could become increasingly difficult to identify and the potential amounts increasingly difficult to store and then interpret.

---

[149] Allitsch, p. 163

If the different types of service providers would have to adhere to similar data retention policies, many of these would have to install entirely new systems to meet the retention requirements. This could be disproportional upon the smaller service providers.[150]

The main question is therefore, is it *practical* to retain all communications data on the off chance that it will be useful one day? In my opinion, the answer will be probably not. As the industry itself put it, "There should not be imposed data storage requirement [on service providers] as this obligation would result in unreasonable high costs or technological impediments and would yield marginal benefits to law enforcement authorities."[151] I think further research is necessary to be able to answer this question affirmatively.

8.3.3 Development of the Information Society

The *e*Europe 2005 Action Plan[152] aims to encourage more effective and efficient interaction between citizens, business and public administration. As much of the information exchanged can be of a personal or confidential nature (medical advise, financial transactions, legal etc),[153] it is vital to ensure the security of such services. One of the policy goals of the Action Plan is to promote growth of e-business and thereby facilitate the creation of jobs and improve productivity.

---

[150] "Communications Data: Report of an Inquiry by the All Party Internet Group" of January 2003, available at www.apig.org.uk/APIGreport.pdf (accessed 25 July 2003)

[151] Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes, 4 June 2003, available at www.eicta.org/dls/common/openFile.asp (accessed 25 July 2003)

[152] Communication from the Commission: eEurope 2005: An information society for all, 28 May 2002, available at http://europa.eu.int/information_society/eeurope/news_library/eeurope2005/index_en.htm (accessed 25 July 2003)

[153] Examples are e-learning, e-government, e-health etc.

If traffic data storage will result in massive costs, this can in turn impact and hamper competition. The risk is that the threshold is too high for new entrants to the markets; smaller service providers will go broke; or new services will not be developed or offered. Large service providers would maybe prefer to establish their headquarters outside Europe in countries where data retention rules are less onerous. Not only private communication, but also business communication would be subject to surveillance by mandatory data retention. Those companies worried about confidentiality of business communication (e.g., in cases of merger acquisitions etc) would maybe choose to use service providers established outside Europe. This will be harmful to the development of the Information Society.

8.3.4 Requests from non-member countries

There may be a certain risk that non-European Union law enforcement authorities will seek data held in Europe that it can not obtain at home, either because it was not retained or because their national law would no permit this kind of access.[154] This could in practice mean that the requested country has to subsidize the cost of preservation and disclosure, to the benefit for foreign law enforcement agencies.

---

[154] See Official Journal of Europe C 155 E/88 3 July 2003, written question E-3081/02 by Erik Meijer (GUE/NGL) to the Commission 28 October 2002: *"Is it possible that, through the exchange of data with Europe, US judicial bodies are trying to obtain traffic data which would not be obtained under US legislation? Does the Commission find it acceptable that, through this circuitous European route, data can be gathered and stored for the benefit of a State which is not authorized to collect such data itself?"* Answer by Mr Liikansen on behalf of the Commission 10 December 2002: *"As suggested by the Honorable Member, the possibility exists that, through obligations imposed within the Union, American authorities get hold of traffic data that would otherwise not be available via their own legal system."*

The requesting country may be charged for any expenses of access and disclosure of data, but the storage cost for service providers – of information that might be requested sometime in the future – will not be recovered. There is also a policy question whether it is desirable that governments may obtain information of their citizens that are not available in their own country.

8.4 Possible solutions

8.4.1 Should anonymisation services be prohibited?

If anonymisation services undermine police work, could one solution be the prohibition of such services,[155] and instead promote the use of pseudonym services. This will grant he citizen "anonymity" in cyberspace, and at the same time provide the necessary data for law enforcement authorities when investigating crimes.

However, this would require that all service providers keep record of their users and log communication traffic. [156] New legislation would be needed to accomplish this.

8.4.2 Obligation to monitor and notify

Would monitoring requirements be less intrusive to the service providers and provide the same results as mandatory data retention? If the service providers were obligated to install filters (e.g. to avoid and/ or report child pornography or racist material) the cost would probably be lower than massive data storage. The benefit is that the spread of illegal material would likely decrease, and the police would immediately gain

---

[155] Note the very strong protection of digital rights management systems (DRMS) and prohibition of circumvention, Directive 2001/29/EC

[156] Inger Marie Sunde: "IKT-kriminalitet: Etterforskningsmetoder og personvern" suggests to introduce a mandatory "e-passport" that registers the identiy of the user when he or she accesses the Internet

knowledge of certain criminal offences.[157] A mandatory requirement to employ electronic agents to detect illegal material would help the police to trace criminal offences, without the privacy concerns that mandatory data retention involves.

In that case, certain articles of Directive 2000/31/EC (as described above) need to be rewritten, and additional legislation must be passed.

8.4.3 Regulation similar in the financial markets

The current situation of service providers has been compared to the former misuse of bank- and financial services for money laundering and illegal financial transactions.[158] Today, data sharing between financial institutions and government agencies has been introduced to increase surveillance of transactions, and there exists a notification obligation when financial institutions gain knowledge of illegal or irregular transactions.

Law enforcement authorities have advocated similar legislation towards those providing communication services.[159]

8.4.4 Data warehouses

It has been suggested that if costs of data storage is to high, service providers should have the option to outsource retention to ”data warehouses” facilitated by government or a Trusted Third Party. [160] Such data warehouses could hold the data from several service providers in a single place, and take responsibility for storage, access and the

---

[157] Though, mandatory data retention was required to prevent crimes like terrorism i.e., and the police will still need traffic data. Terrorism will not be “filtered” away.

[158] Inger Marie Sunde,: ”IKT-kriminalitet: Etterforskningsmetoder og Personvern” and ”Telekombransjens rolle i moderne kriminalitetsutvikling”

[159] Ibid.

[160] E.g., a private contractor or entity authorized by government and/ or consumer interest organizations

subsequent deletion of data. The Industry, however, thought that this would not be lawful or desirable, and Foundation for Information Policy Report (FIPR) has claimed that data warehouses are exactly the tools needed to create a totalitarian state.[161]
A danger is that such warehouses could be attractive targets for hackers that wants data for totally different purposes that crime investigation.

8.4.5 Suggestion of how to carry out mandatory data retention

From the discussion above, it seems safe to conclude that everyone agrees with the following:

- Fundamental human rights and freedoms must be secured
- Every individual has a right to privacy
- Victims of computer crime have a right to protection.[162]

A possible solution could therefore be:

- Requirement of data retention for a fixed period of time, of very clear and narrowly defined traffic data
- Detailed description of the procedures for storage and maintenance
- Access to stored traffic data should be restricted exclusively to law enforcement authorities for crime investigation purposes
- Close evaluation of the measures over a period of 5 years, to ensure the requirements fulfils their purpose and does not jeopardize the privacy of individuals. Necessary adjustments or amendments may be made.

In this way, consensus may be reached on the important issues of data preservation and data retention as a compromise between the different interests at stake.

---

[161] Quoted in AGIP Report, p. 24

[162] G8 Report

8.4.6 Fines

An additional solution would be to impose fines for misuse of traffic data information. If law enforcement authorities use traffic data where the suspicion against a person is not correct, the person may claim damages. The fines should be quite high, to avoid any situations where data are misused, or used for other purposes than crime investigation and prosecution. This would ensure that the police get a judicial order for access to data in specific cases, and the service providers (or whoever stores the data, cf. data warehouses) need to control the access and that data is not used for other purposes by private entities.

9 Concluding remarks

Further analysis of the costs (i.e., both privacy costs and economic costs) and benefits of data retention would be preferrable. This includes the number of cases solved because of access to traffic data, and cases left unsolved due to lack of such data. Until reliable statistics of the current situations are available, it is difficult to conclude whether data retention should be made mandatory or not.

Data retention is an intrusive measure that will impact both the individuals' right to privacy and the development of the Information Society. The principle of proportionality calls for the less intrusive measure (i.e., data preservation) to be tried out first. The Cybercrime Convention will ensure that contracting Parties implement preservation requirements in national laws. Only if the provisions of data preservation fail to be sufficient to the aim pursued, more intrusive measures such as data retention can be jusitified.

However, there is a demonstrable need for access to traffic data in crime investigations. The situation where no data is available because they are not registered (e.g., anonymous Internet surfing, flat rate billing) will not be solved by any preservation or retention requirements. The issue needs to be addressed separately, and the need for new legislation in this area should be considered.

Nobody wants cyber criminals to go unpunished. The challenge is to find the right balance between the different interests involved.

10 References

10.1 Treaties/ Statutes/ Guidelines

Council of Europe Convention on Cybercrime (ETS no. 185, Budapest 23.XI.2001)

Council of Europe – Explanatory Report to the Convention on Cybercrime (ETS No. 185)

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist or xenophobic nature committed through computer systems (ETS No. 189)

Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (ETS 108, Strasbourg 28.I.1981)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data (Data Protection Directive)

Directive 97/66/EC of The European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (Directive on privacy in the telecommunications sector)

Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and electronic communications)

Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

Organization for Economic Co-operation and Development (OECD) Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data, 23 September 1980

United Nations (UN) Guidelines concerning computerized personal data files, 14 December 1990

10.2 Recommendations

Recommendation No. (89) on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes

Recommendation No. (95) concerning problems of criminal procedural law connected with information technology

10.3 Literature/ Reports/ Articles

AGIP- Submission on behalf of UK Law Enforcement, available at http://www.apig.org.uk/lea.pdf (accessed 25 July 2003)

Answers to questionnaire on traffic data retention, by Council of Europe 20 November 2002, available http://www.effi.org/sananvapaus/eu-2002-11-20.html (accessed 25 July 2003)

Allitsch, Rainer: "Data Retention on the Internet – A measure with one foot offside?" *CRI* 6/2002

Blume, Peter: "Overvågning af og i cyberspace", *Fra rådet til tinget,* No. 166 (2002) pp.3-6

Bygrave, Lee A.: *Data Protection – Approaching Its Rationale, Logic and Limits* (The Hague/Boston/London: Kluwer Law International, 2002)

____ "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties" *International Journal of Law and Information Technology*, Volume 6, (1998), pp. 247-284

Clarke, Roger: "A Primer on Internet Technology" (1997) Version of 15 February Xamax Consultancy Ptd Ltd, *Additional material, Masters of Law (Oslo: NRCCL, 2003)*

Communication from the Commission: eEurope 2005: An information society for all, 28 May 2002, available at http://europa.eu.int/information_society/eeurope/news_library/eeurope2005/index_en.htm (accessed 25 July 2003)

Electronic Privacy Information Centre, "Privacy and Human Rights 2002 – An International Survey of Privacy Laws and Developments" (Washington DC, 2002), available at www.privacy.org/pi/survey/phr2002/phr2002-part1.pdf (accessed 25 July 2003)

EU COM (2000) 890 final: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, Brussels, 2 January 2001, available at http://europa.eu.int/ISPO/eif/internetpoliciessite/crime/crimecommEN.html (accessed 25 July 2003)

EU Forum on Cybercrime, *Discussion Paper for Expert's meeting on Retention of Traffic Data*, 6 November 2001 (informal working paper prepared by the Commission services), available at

http://europa.eu.int/information_society/topic/telecoms/internet/crime/wpap1ov/index_en.htm (accessed 25 July 2003)

Fuhr, Ringdal & Mørkved: "Etterforskning av telekommunikasjon: Loven krever fritak fra taushetsplikten", published in *Juristkontakt* 2/3003

Goodman, Marc D. & Brenner, Susan W.: "The Emerging Consensus on Criminal Conduct in Cyberspace" *International Journal of Law and Information Technology*, Oxford: Oxford University Press 2002

G8 Government-Private Sector High-Level Meeting On High-Tech Crime, Report for Workshop 1: Data Retention Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, Tokyo, 22-24 May, 2001, available at www.mofa.go.jp/policy/i_crime/high_tec/conf0105-4.thml (accessed 25 July 2003)

Julia-Barcelo, Rosa: "Liability for on-line intermediaries: comparing EU and US legal frameworks" in Unipub AS', *Required reading Part I, E-commerce law, Masters of Law* (Oslo: Kopinor, 2003)

Koelman, Kamiel J.: "Online Intermediary Liability" in Unipub AS', *Required reading Part I, E-commerce law, Masters of Law* (Oslo: Kopinor, 2003)

Morris, Daniel A.: "Tracking a Computer Hacker", available at www.cybercrime.gov (accessed 25 July 2003)

National Strategy to Secure Cyberspace, available at http://www.whitehouse.gov/pcipb/ (accessed 25 July 2003)

Robinson, James K.: "Internet as the Scene of Crime" speech at the International Computer Crime Conference, Oslo, Norway, May 29-31, 2000, available at www.cybercrime.gov (accessed 25 July 2003)

Sieber, Ulrich: "Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME Study" (1998), available at http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc (accessed 25 July 2003)

Statewatch: "Surveillance of communications, Data Retention to be Compulsory" Volume12 no 3 / 4 May-July 2002, available at www.statewatch.org/neww/2002/aug/05datafd1.htm (accessed 25 July 2003)

Sunde, Inger Marie: "Online Crime – Bevisførsel og strafferammer i datakrimsaker" published in *Rett & Slett* nr 1, 2000, available at www.okokrim/datakrimsenteret/artikler (accessed 25 July 2003)

___"Convention on Cybercrime" published in *Tidsskrift for strafferett* 1/2002, available at www.okokrim/datakrimsenteret/artikler (accessed 25 July 2003)

___"IKT-kriminalitet: Etterforskningsmetoder og Personvern", n.d., available at www.okokrim/datakrimsenteret/artikler (accessed 25 July 2003)

___"Telekombransjens rolle i moderne kriminalitetsutvikling", published in *Teknisk Ukeblad* no 5, 3. februar 2000, available at www.okokrim/datakrimsenteret/artikler (accessed 25 July 2003)

The Computer Related Crime Research Unit, "Study on the legal issues relevant to combating criminal activities perpetrated through electronic communications – Final Report" (London, 2000), available at http://europa.eu.int/ISPO/eif/internetpoliciessite/crime/study2000/cover.html (accessed 25 July 2003)

Trimidas, Takis, *The General Principles of EC Law,* (New York: Oxford University Press, 1999)

10.4 Statements

"Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes" of 4 June 2003 by ICC, UNICE, EICTA and INTUG, available at http://www.iccwbo.org/home/menu_electronic_business.asp (accessed 25 July 2003)

"Communications Data: Report of an Inquiry by the All Party Internet Group" of January 2003, available at www.apig.org.uk/APIGreport.pdf (accessed 25 July 2003)

Statement of the European Data Protection Commissioners 11 September 2002, published at the website of Foundation for Information Policy Research (FIPR), available at http://www.fipr.org/press/020911DataCommissioners.html (accessed 25 July 2003)

Statement of the European Data Protection Commissioners 11 September 2002, published at the website of Foundation for Information Policy Research (FIPR), available at http://www.fipr.org/press/020911DataCommissioners.html (accessed 25 July 2003)

April-May 2002 Campaign against data retention: Open letter to Pat Cox, President of the European Parliament 22 May 2002. Available at http://www.epic.org/privacy/intl/data_retention.html#humanrights (accessed 25 July 2003)

Annex I

G8 Government-Private Sector High-Level Meeting On High-Tech Crime, Report for Workshop 1: Data Retention Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, Tokyo, 22-24 May, 2001

Appendix A to Report of Workshop 1a

The following is a list of log details related to some services that may be available to an Internet service. It should be noted that the content of these logs might be subject to relevant business, technical and legal conditions; not all of the following data elements will be available in all logs.

(1) Network Access Systems (NAS)
- access logs specific to authentication and authorization servers such as TACACS+ or RADIUS (Remote Authentication Dial in User Service) used to control access to IP routers or network access servers.

- date and time of connection of client to server[1]

- userid

- assigned IP address

- NAS IP address

- Number of bytes transmitted and received

- Caller Line Identification (CLI)[2]

(2) Email servers
- SMTP (Simple Mail Transfer Protocol) log

- date and time of connection of client to server

  - IP address of sending computer

  - Message ID (msgid)

  - sender (login@domain);

  - receiver (login@domain)

  - status indicator

POP (Post Office Protocol) log or IMAP (Internet Message Access Protocol) log

- date and time of connection of client to server

- IP address of client connected to server

- Userid

- In some cases identifying information of email retrieved

(3) File upload and download servers
- FTP (File Transfer Protocol) log

- date and time of connection of client to server

- IP source address

- userid

- path and filename of data object uploaded or downloaded

(4) Web servers
- HTTP (HyperText Transfer Protocol) log

- date and time of connection of client to server

- IP source address

- operation (i.e., GET command)

- path of the operation (to retrieve html page or image file)

- "last visited page"

- response codes

(5) Usenet
- NNTP (Network News Transfer Protocol) log

- date and time of connection of client to server

- protocol process ID (nnrpd[NNN...N])

- hostname (DNS name of assigned dynamic IP address)

- basic client activity (no content)

- posted message ID

(6) Internet Relay Chat
- IRC log

- date and time of connection of client to server

- duration of session

- nickname used during IRC connection

- hostname and/or IP address

(Note)

1 Reliable time records among different computers and networks is essential for investigation and prosecution. The use of the Network Time Protocol (NTP) for synchronization should be an ISP Best Practice.

2 CLI provides the number from which a telephone call is made and may or may not be available to ISPs. CLI retrieval is specific to the given combination of software and hardware.